The Future of the Internet

The DoD Globalization Task Force Staff

The Internet's continuing growth, stability, and security are vital to the DoD's mission. While the DoD no longer controls Internet decision making, its unique perspective deriving from its multiple roles as Internet user, operator, and research center is important to the development and protection of U.S. national interests. It should make a commitment to participate directly in international Internet decision-making forums, as well as actively develop policy as part of the U.S. interagency process.

The Internet is essential. It is a vital underpinning of the civilian economy, and its security and stability has become a matter of national security. In a converged world, it will become not just the means for transmitting data, but also video and voice. It is, therefore, critical to ensure its continued growth, internal security, and stability.

So how do we guarantee that growth, security, and stability? What might impact those issues? Who gets to make those decisions?

The USG, through the DoD, created the Internet, but what it created has grown in ways totally unforeseen just 10-15 years ago. The DoD's oversight of the initial development of the Internet has been replaced by a web of collective decision-making bodies that it no longer controls. The issue now has become should the DoD continue to try to influence the development of the Internet and, if so, how should it proceed? That is, should the DoD take an active role in the process and, if it should, will that role be confined to internal USG deliberations or will it include direct participation in the many forums where key decisions about the Internet are made?

The rest of this article answers that question as follows: the DoD finds itself in a unique position to play a positive role. It is a major user of the Internet, but it is also a large Internet service provider and an operator of two of the 13 root zone servers that provide the basic information for locating Internet addresses. The DoD is also a repository of vast technical expertise about the Internet and a significant source of research funds. Taken together, those multiple roles give the DoD a unique view of the Internet and a distinct ability to positively influence its evolution in ways not easily matched by other USG departments or the private sector.

Those perspectives – individually and in combination – are critical for the DoD to carry out its larger mission: assuring the security and stability of the Internet as part of its defense of U.S. national security. The DoD's strategy should be twofold. It must (1) monitor and influence current technical and political developments that could impact the security and stability of Internet operations; and (2) envision the Internet 10 or 15 years into the future, define the role it will play in contributing to the defense of the nation, and take the steps required to achieve that vision, much as the defense community has done with the current Internet.

However, the DoD's distinct vision does not mean that it can afford to act alone. In order to make the DoD's participation effective, there will have to be a coordinated strategy among the DoD's components, as well as collaboration with the rest of the USG and the U.S. private sector. That collaboration is not driven merely by the desire to speak with one voice. Rather, it is compelled by the unique set of problems and unique ways of solving them that distinguish the Internet and its governance processes.

Collective decision-making about the Internet is disbursed among various organizations and, in most of them, governments have no special role. They stand on equal footing with the private sector, academia and civil society in devising standards and making other relevant decisions. It is a *megacommunity*[1] of extraordinary scope with vast and complicated interests and connections.

Moreover, the decision makers must constantly struggle to preserve the Internet's grassroots innovation and growth while recognizing the importance of stability and security. The creativity that has made the Internet so valuable cannot be squelched if the Internet is to remain a dynamic and adaptive medium. Continuing to achieve that balance of innovation and stability requires a combination of technological expertise, political sophistication, and a commitment to innovation and change that few individuals, let alone agencies, possess. It is the combination of perspectives from within and outside of government that, if successfully executed, gives the USG both compelling influence and a powerful vision.

The Questions

The following questions are integral to an Internet Governance and Security Strategy for the defense community:

- What should the Internet look like in 10 or 20 years to ensure it remains a secure link to our allies, the defense community global supply chain, and the civilian infrastructure on which the USG depends?
- What should the Internet look like in 10 or 20 years to maximize its ability to support other USG interests?
- What steps should the national security community take today to ensure that the security and stability of the Internet's infrastructure are protected to support future operations? From a policy standpoint (i.e., global, national, DoD)? From an investment standpoint (e.g., resourcing, research and development)? From a cultural standpoint (e.g., training, education)? From a tactical standpoint (e.g., standards, operations, acquisitions)?

The Trends

One can likely come up with a variety of ways of categorizing the various challenges for the Internet. The following are three that are seen as summarizing the diverse problems:

1. The rapid *growth* of Internet services and, therefore, Internet traffic because of the increasingly essential character of the Internet for national and international economies (all of which makes the Internet not just a bigger target, but also a more inviting one, as well).

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Future of the Internet	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **DoD Globalization Task Force Washington, D.C. 20301-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
CROSSTALK The Journal of Defense Software Engineering July 2008

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**7**	

2. The growing sophistication of those who want to destroy the Internet's *stability and security*, whether for reasons of cyber-war, crime, or simple malicious one-upmanship.
3. The increasing demands placed on those *organizations* that make decisions related to standards and practices governing the Internet.

Growth

First, with regard to growth, the trends are overwhelming:

- Everything will be over Internet Protocol (IP) (Voice over IP [VoIP], video, streaming video, collaboration, data), which means systems will bear vastly greater amounts of traffic.
- Everything will be addressable via IP addresses (sensors, mission-critical systems, individuals, etc.).
- There will be vast numbers of new uses which will have implications on the volume of traffic and privacy of data, among other things.
- The Internet will be more intelligent and interactive.

That growth suggests a responsive agenda that should address the following areas:

1. **Scale/Ubiquity**. The more Internet traffic, the greater the threat of congestion and packet loss. The greater the congestion, the greater the interference with VoIP and video. Unlike data where we have learned to tolerate the time it sometimes takes for things to appear on computer screens (as we expectantly peer at our monitors), video and VoIP transmissions cannot be delayed or disrupted without substantially degrading service (which is referred to as the problem of *latency*). There are also questions of whether computational capacity on root zone servers can meet demand, and whether the constant updating of routing tables will strain the routers' computational ability. The routing schemes will need to account for more routers and links, and quality of service (a term related to the issue of *net neutrality*, discussed in the third area, Quality of Service) will complicate their work. Modifications to the current global routing scheme will be required to support controlled peering among networks, and routing protocols will need a complete system view of options (rather than a partial view focused on the next jump). There is also the question of whether increasing capacity requirements will be met with current technologies.
2. **Resiliency.** Ubiquitous VoIP and similar high bandwidth, low latency applications, as well as increasing dependence on the Internet for mission-critical operations, require a more reliable and robust system. In the face of major man-made or natural disasters or deliberate attacks on the system, will there be enough robustness, redundancy, and accurate routing and address information to assure continued connectivity and speed? In addition, exchange point technology needs to be improved and there are robustness issues at major interconnection points including, among other things, a lack of redundancy.
3. **Quality of Service – Net Neutrality and Priority of Service.** On traditional telephone networks, carriers have evolved protocols for priority communications, a particularly important issue for national security and law enforcement. Thus far, the Internet has worked on a *best efforts* basis where all traffic is essentially treated the same. With more traffic and potential limits on capacity, it is important to ensure similar priority schemes. However, some commercial users are worried about possible abuse of priority schemes by service providers to discriminate in favor of some content or services over others. They have proposed net neutrality laws that could interfere with the ability to prioritize communications for national security/emergency preparedness purposes. The White House has stated that it sees no reason for net neutrality legislation; that the market will work itself out [1]. The Federal Communications Commission (FCC) is currently reviewing net neutrality through a notice of inquiry[2], and holding hearings on the issue in light of evidence that carriers may have been violating net neutrality principles.
4. **IPv6 Deployment.** As a result of the growth of the Internet, the addressing system must be expanded. IPv6 is a new addressing system that allows for billions more potential addresses than the current system, IPv4. Both the USG and private industry must be prepared for the transition to ensure that it occurs smoothly and that all IP addresses remain reachable. Because of the relatively large number of addresses that remain available in the U.S., there has thus far been little interest here in undertaking the necessary investment, even though the Office of Management and Budget has directed all USG agencies to complete the transition by June 2008[3]. While the DoD has moved forward, many U.S. agencies have not. However, the rest of the world is likely to want to push forward in the near future. At that point, the U.S. may have no choice; however, timely addressing of the transition is the best way to avoid a crisis.
5. **Alternative Technologies.** The National Academy of Sciences has noted that Internet research at this point is heavily incremental in nature, focusing on marginal improvements to the current structure.[4] There is little money or effort devoted to changing the fundamentals of the Internet. Regardless, there is always the possibility that some alternative technology will come along that will make the Internet outmoded in the same way the Internet has begun to make the Public Switched Telephone Network (PSTN) virtually obsolete. If funded, the National Science Foundation Global Environment for Network Innovations project[5], with which the DoD (principally through the

... some commercial users are worried about possible abuse of priority schemes by service providers to discriminate in favor of some content or services over others ... The White House has stated that it sees no reason for net neutrality legislation; that the market will work itself out.

Defense Advanced Research Projects Agency [DARPA]) collaborates, will investigate new core functionality, new architectures and new network architecture theories, and build higher-level service abstractions.

6. **Web 2.0.** Some issues of growth relate to the evolution of Internet applications. The increasing sophistication of highly interactive Internet applications, often collectively referred to as Web 2.0, provide users with an expanding range of capabilities.[6] The DoD can and does use them, but the value to the DoD is nowhere as significant as the capability they afford non-nation state actors – such as terrorists – to use new and innovative ways to train terrorists (e.g., avatars), share information, recruit followers, and otherwise enhance their ability to conduct asymmetric warfare.

For all these issues, the DoD's perspective is extraordinary. It is the user who has a direct interest in all these problems, but it is far more than that. For example, it is an Internet service provider that has to adopt IPv6, and it is a research funding source that can influence long-term events. If all parts of the DoD are talking to one another, then it is a *feedback loop* unparalleled in the Internet world.

Stability and Security

If growth is deemed a *good* trend, then the second trend, the increasing sophistication of hackers, criminals, and state-sponsored cyber-warriors clearly represents the *bad* side of the following equation:

- Identity theft, fraud, unwanted e-mail, and other Internet abuses continue to grow.
- Because the Internet can originate virtually anywhere and can easily penetrate a national boundary, cyber-crime is both everywhere and nowhere all at the same time.
- Cyber-attackers have learned to manipulate hundreds, sometimes thousands, of computers to conduct coordinated attacks on a computer system (called *botnets*). These botnets have significantly facilitated large, broad-scale attacks on computer networks called distributed denial of service attacks (DDOS).
- In 2007, a large-scale attack on Estonia demonstrated the ability of sophisticated parties to disrupt large parts of a national economy through the use of DDOS.[7]
- The international world has been unable to agree on what cyber-crime is or how to deal with those who commit it. The Internet Cyber-Crime Convention has been signed by only 43 countries, including the United States. Russia, China, North Korea, and many others have not signed.

There are many possible responses to these problems, but the following are clear priorities:

1. **DDOS.** DDOS attacks are increasingly being used to conduct attacks against key Internet assets including the Internet's root zone servers.

The BGP is used to perform inter-domain routing on the Internet and is vulnerable to spoofing and misconfiguration, which can lead to the misrouting of Internet traffic.

These DDOS attacks attempt to overwhelm servers with vast numbers of messages. The use of botnets has increased the effectiveness of DDOS attacks. The last major attack in the U.S. occurred on February 6, 2007. Its impact was heavily mitigated by the use of anycast technology, which, by duplicating root zone data bases on multiple servers around the world, allowed traffic to be re-directed around the victimized servers. However, the attackers are also growing more sophisticated, and the need for ever-more elaborate defense continues to grow. Mitigation approaches include bandwidth upgrades, ingress and egress filtering, and mandatory hardware configuration to eliminate the possibility that computers could be taken over by unauthorized users. One sign of the seriousness of the problem is that Internet service providers are considering the cost effectiveness of accepting only traffic from known entities. However, this approach could block access to online sites and eliminate the end-to-end nature of the Internet. Government and private industry will need to continue to work closely to address this issue from both a policy and operational perspective.

2. **Defining Cyber-War and Cyber-Conflict.** The Estonia situation showed the difficulties present in defining cyber-conflict. Although a nation-state was suspected of causing the DDOS attacks against Estonia's key Web resources, it was difficult to trace ultimate culpability. In addition, there was a question of whether this type of denial of service would be considered a cyber-incident of national significance considering the fact that it caused more annoyance than actual harm. Although the Estonia situation seemed to bring attention to the fact that nation-state strategic cyber activity might be on the rise, it equally brought light to the fact that cyber rules of engagement have yet to be defined. Much work will have to be done in the next decade defining international law and norms of behavior, by treaty or other means, to ensure that the Internet will survive in light of a rise in nation-state cyber conflict.
3. **Authentication (Public Key Infrastructure/Domain Name System [DNS] Security Extension [DNSSEC] Deployment).** To ensure secure and stable Internet communications, it is essential that Internet users have confidence that they are communicating with the parties with whom they intend. For the Internet to complete its evolution into the key platform for all types of communications, there must be confidence that the global network infrastructure is secure and reliable. Users must continue to be able to trust that they are communicating with the people they intend to communicate with, that they are doing so in a timely fashion, and that the data, video, or voice calls they are sending or receiving remain confidential and their integrity is protected.

An essential element in assuring this security is that domain names have a trustworthy mapping to IP addresses and are not tampered with or disrupted. DNSSEC authenticates communications through the use of *public keys* bound to a unique user to

ensure that IP addressing is authentic and accurate. It should be integrated into the Internet to provide for assured distribution of IP addresses and autonomous system numbers. DNSSEC would validate DNS addresses and deter spoofing of Web sites (thereby allowing communications to be misdirected) and other Internet services. Signing the Internet's root zone files (the Internet Assigned Numbers Authority [IANA] root) and the roots for the Top Level Domains (TLDs) would also improve Internet integrity.

4. **Routing Security (Border Gateway Protocol [BGP]; Router Upgrades).** As noted in the discussion of Internet growth, the increase in Internet traffic raises questions of whether computational capacity on root zone servers can meet demand, and whether the constant updating of routing tables will strain the routers' computational ability. The BGP is used to perform interdomain routing on the Internet and is vulnerable to spoofing and misconfiguration, which can lead to the misrouting of Internet traffic. While technologies to increase BGP security, such as Secure BGP and Secure Origin BGP, exist to protect against BGP vulnerabilities, they are expensive, require widespread implementation, and have not been widely adopted by the community. Ultimately, operators will have to step up to the cost or figure out an alternative that eliminates the problem.
5. **Out-of-Band Control Space for the Internet.** The PSTN relies on a parallel, out-of-band network (the SS7 network), to separate telecommunications content from operational control messages. This parallel, out-of-band management approach vastly increases the security and reliability of the PSTN network. Current Internet architecture does not permit out-of-band management of the Internet control space where both communications content and message control information are sent over the same network at the same time. This subjects Internet traffic flow to the risk of tampering and corruption. An out-of-band control space for the Internet could greatly improve the ability to isolate network management data and increase reliability.

Each of these issues has already drawn USG attention. USG reliance on the Internet, or on other agencies and businesses that rely upon the Internet, make the Internet a target for any opponent. The fact that a few highly qualified individuals can create significant trouble in this environment merely underscores the attractiveness of targeting the Internet as a tool of asymmetric warfare in which terrorists as well as nation states can engage.

Organizations

The third trend, changes in how the Internet is governed, simply complicates how to deal with the first two trends.

- The U.S. has had considerable influence over how the Internet has been governed, but that influence is now likely to wane for several reasons. First, as the Internet becomes more embedded around the world, the technical expertise that once resided largely, if not exclusively, in the United States is becoming dispersed. Second, the creators of the Internet, many of whom were once employed by the USG and who, through its prestige, history, and expertise continue to have considerable influence in the various governance forums, are now retiring. Third, virtually all governments now recognize the importance of the Internet for economic reasons, and there is universal appreciation of the Internet's capability to enhance free speech – a positive value to many nations but a threat to others. For one reason or another (or both), some governments now want to control Internet decision-making. They seek to displace the private sector, which has largely had control over key Internet-related decisions for the past two decades as a result of U.S. policy in favor of such control. Similarly, some want to displace the role of the United States, which maintains some limited control by its agreements with the Internet Corporation for Assigned Names and Numbers (ICANN) and the IANA, both of which play a role in the domain name system that assigns Internet addresses and authorizes TLDs (such as .com).
- The American private sector, on which the USG has relied to represent its interests because of their close alignment on most significant Internet policy questions, is growing increasingly globalized. The close working relationship may not be sustainable in that environment.

IANA would be the logical holder of the public part of the signed root key, but its connection with the USG raises serious objections in some quarters from those who claim to fear that the USG could use its influence to disrupt traffic to and from countries it opposes.

The responses to these challenges are both short- and long-term:

1. **Resolving the Status of ICANN.** The USG, through the Department of Commerce (DoC), created ICANN in 1998 and contracted with it to operate IANA, which performs vital IP addressing functions, including maintaining the domain addresses on the Internet's 13 root zone servers (and more than 100 anycast clones). Since then, the DoC has maintained a Memorandum of Understanding (now a Joint Project Agreement [JPA]) with ICANN, the purpose of which is to ensure that ICANN would become sufficiently democratic, transparent, accountable, and efficient so that it could be allowed to fully privatize. The current JPA ends in 2009, and the DoC has received comments in response to a Notice of Inquiry as a mid-term review regarding ICANN's status in becoming secure and stable organization.[8] The problem is complex: not only is there the issue of whether ICANN has met its goals, but also there is the problem of whether a fully privatized structure can be guaranteed protection from other governments' attempts to exercise unwanted influence over its operations. Although there is no equivalent issue with regard to IANA, with which the USG has not promised to eventually terminate its contract, other governments contin-

ue to press for a change in IANA's status. The dispute has other ramifications. IANA would be the logical holder of the public part of the signed root key, but its connection with the USG raises serious objections in some quarters from those who claim to fear that the USG could use its influence to disrupt traffic to and from countries it opposes.

2. **Defining the Role of the International Telecommunication Union (ITU).** The ITU is a United Nations-related agency that, for many decades, has been the principal international forum for standards related to telephone service.[9] It is also the only significant organization related to Internet governance where governments are the sole voting parties. The ITU has long played a role with regard to the Internet. Because the Internet is carried over telephone networks, standards related to those networks' involvement in the Internet are often addressed by the ITU. However, some governments see the ITU as a way to extend their influence over Internet decision-making and, therefore, are pressing for an expansion of the ITU's role in Internet-related issues. The ITU's leadership seems open to some of these ideas. The Secretary General of the ITU recently told a gathering in Washington, D.C., that he would consider having ICANN's government advisory committee become a function of the ITU. Some of those questions are likely to be addressed during the World Telecommunications Standards Assembly, to be held later this year, and the World Telecommunications Policy Forum scheduled for 2009.
3. **Artificial Intelligence as a Substitute for Organizational Control.** Those who control the technical hierarchies and centralized nodes of the Internet also hold greatest power over the network and, ultimately, its users. There needs to be research to explore the possible reconfiguration of the DNS protocols and any other infrastructure tools that are inherently hierarchical or centralized in nature with a view toward eliminating as many technical points as possible that require human decision-making. Research should also be conducted to determine whether changes in protocols and use of artificial intelligence at key decision points, together with increased use of mirroring, open architectures, and other transparencies would enable greater overall system adjustments via competitive market forces rather than through organizations, such as ICANN, which would reduce the pressure for increased political control.

The Way Forward

The way forward must focus on research and representation. There are a variety of defense organizations that fund projects that address the evolutionary aspects of Internet R&D or alternative technologies, including the Army, the Naval Research Labs, and DARPA. DARPA recently released a Request for Information for Assurable Global Networking, suggesting a renewed interest from DARPA in alternate technologies. Part of their work involves participating in the White House's Office of Science and Technology Policy's Networking and Information Technology Research and Development program, which is the result of the High-Performance Computing Act of 1991, 105 Stat. 1594, and the Next Generation Research Act of 1998, 112 Stat. 219.[10]

The challenge for the DoD is assuring the continued coordination of all this work to ensure security and stability within the fast-changing Internet and the increasing capabilities of those attacking its security and stability. The needs of the GIG are driving some of this activity, as are the tactical and strategic concerns surrounding terrorist and nation-state use of the Internet against our national security interests. The National Defense University will shortly publish an extensive report on *cyber power* that may help facilitate the discussion, but developments happen so quickly that the discussion must be constant and intense. The evolving recognition of the significance of the challenge and its broader implications for national security should push current activity to an even higher level.

Similarly, the DoD currently participates in some organizations that are involved in Internet-related decision-making. As the operator of .mil, the DoD tracks activity in the American Registry for Internet Numbers, the Regional Internet Registry for North America, and parts of the Caribbean. The DoD also monitors developments in the Internet Engineering Task Force (IETF), which sets standards for core

Internet functions, and the related Internet society. The DoD has regularly been active at the ITU, although with a greater focus on the wireless spectrum rather than the Internet. In many cases, the DoD has only had the ability to monitor developments, and not to drive activity or offer leadership in these organizations that are reputation-based and require active and sustained participation.

The continuing challenge is to coordinate all of these activities within the DoD, with the rest of the USG, and with the American private sector. The ability to influence cannot rest solely on one's government status. Even at the ITU, where governments control the votes, key policy decisions about telephone networks are made in the study groups where the private sector dominates. Influence there is dependent on constant and highly competent participation by individuals. The same is true at ICANN and the IETF. Hence, the DoD's ability to analyze issues based on its vast technical insights, its needs as a user, and its status as an Internet service provider give it a unique ability to work in these environments. Other agencies have important roles to play, but their work can be powerfully enhanced by committed DoD support.◆

Reference

1. Wired.com. "Bush Administration Restates Position on Proposed Internet Traffic Policing Rules." Wired.com. Sept. 2007 <http://blog.wired.com/27bstroke6/2007/09/bush-administra.html>.

Notes

1. A megacommunity is defined and referenced as the following:

> ... a public sphere in which organizations and people deliberately join together around a compelling issue of mutual importance, following a set of practices and principles that will make it easier for them to achieve results. Like a business environment, a megacommunity contains organizations that sometimes compete and sometimes collaborate. But a ... megacommunity is a larger ongoing sphere of interest, where governments, corporations, non-governmental organizations, and others intersect over time. The participants remain interdependent because their common interest compels them to work together, even though they might not see or describe their mutual problem or situation in the same way.
>
> Booz Allen Hamilton. The Megacommunity Way: Mastering Dynamic Challenges With Cross-Boundary Leadership. July 2007 <www.boozallen.com/publications/article/38632762>.

2. FCC Notice of Inquiry. In the Matter of Broadband Industry Practices. WC Docket No. 07-52, adopted 22 Mar. 2007.
3. Office of Management and Budget. "Memorandum for Chief Information Officers." Transition Planning for Internet Protocol Version 6 (IPv6). 2 Aug. 2005 <www.whitehouse.gov/omb/memoranda/fy2005/m-05.22.pdf>.
4. Lucky, Robert, and Jon Eisenberg, eds. Renewing U.S. Telecommunications Research. National Academies Press, 2006.
5. See <www.geni.net>.
6. For a further explanation of this concept, see Tim O'Reilly's Web site <www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/what-is-web20.html>.
7. Traynor, Ian. "Russia Accused of Unleashing Cyberwar." The Guardian 17 May 2007 <www.guardian.co.uk/world/2007/may17/topstories3.russia>.
8. NTIA. "Statement of the Mid-Term Review of the Joint Project Agreement (JPA) Between NTIA and ICANN." 1 Apr. 2008.
9. See <www.itu.int>.
10. See 15 USC Sec. 5501 et. seq. for the text in the U.S. Code.

Additional Reading

1. Loren Data Corp. "A Military Networking Technology for Global Information Exchange." FedBizOpps 13 Sept. 2007 <www.fbodaily.com>.
2. Hayes, Frank. "Frankly Speaking: Pakistan's BGP Sabotage Bodes Ill for IT." Computerworld 3 Mar. 2008 <www.computerworld.com>.
3. Karlin, Josh, Stephanie Forrest, and Jennifer Rexford. Pretty Good BGP: Improving BGP By Cautiously Adopting Routes. University of New Mexico Technical Report TR-CS-2006-10, June 2006 <www.cs.princeton.edu/~jrex/papers/pgbgp.pdf>.
4. Agence France-Press. "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-Attacks." The RawStory.com. 15 May 2007 <http://rawstory.com/news/afp/Estonia_urges_firm_EU_NATO_response_05152007.html>.
5. Gross, Grant. "ICANN Looks Toward End of U.S. Agreement." IDG News Services 7 Mar. 2008 <www.infoworld.com/article/08/03/07/ICANN-looks-toward-end-of-US-agreement_1.html>.

About the Author

Mitchell Komaroff leads and is the Acting Director of the Globalization Task Force (GTF), for the ASD(NII)/DoD CIO. The GTF is an office within the Office of the DoD CIO dedicated to strategic national security planning to address risks arising from the globalization of the telecommunications infrastructure and of the marketplace for information and communications technology. He is primarily responsible for developing and implementing a strategy for mitigating national security risks to DoD arising from the increasing globalization of the ICT sector. The GTF is the ASD (NII)/DoD CIO focal point for transactional risk management in Committee on Foreign Investment in the U.S. and FCC licensing matters, developing strategies for preserving and improving Internet security and stability in support of DoD and USG communications, and policy development addressing global supply chain risk. Komaroff has worked to implement software and systems assurance across the DoD. He has worked previously as a computer scientist with DISA, and with industry where he worked network quality of service, IA architecture, and information management issues. Komaroff holds a master's degree in mathematics from George Mason University and a Juris Doctor degree from the University of Maryland, School of Law.

Phone: (703) 697-3314
E-mail: mitchell.komaroff@osd.mil

Acronym Key for This Issue

AIS: Assured Information Sharing
C&A: Certification and Accreditation
CIO: Chief Information Officer
CNSS: Committee on National Security Systems
DASD(IIA): Deputy Assistant Secretary of Defense for Information and Identity Assurance
DIACAP: DoD Information Assurance Certification and Accreditation Process
DIAP: Defense Information Assurance Program
DISA: Defense Information Systems Agency
DNI: Director of National Intelligence
DoD: Department of Defense
GIAP: GIG IA Portfolio (Management)
GIG: Global Information Grid
IA: Information Assurance
IC: Intelligence Community
INFOSEC: Information Security
IT: Information Technology
NII: Networks and Information Integration
NSA: National Security Agency
NSS: National Security Strategy
R&D: Research and Development
SME: Subject Matter Expert
UCDMO: Unified Cross Domain Management Office
USG: United States Government